PhD
FINAL ORAL EXAMINATION

Tuesday, April 5th
3:10p.m. @ Snedecor 2113

Jinsheng Zhang

Faculty Advisor: Professor Wensheng Zhang

Data Access Pattern Protection in Cloud Storage

Cloud-based storage service has been popular nowadays. Due to the convenience and unprecedent cost-effectiveness, more and more individuals and organizations have utilized cloud storage servers to host their data. However, the cloud servers can be hacked and may not be fully trustable. As found by Islam et. al., data encryption alone is not sufficient. The server is still able to infer private information from the user's. Therefore, Oblivious RAMs (ORAM) have been proposed to allow a user to access the exported data while preserving user's data access pattern. In recent years, many ORAM constructions have been proposed to improve the performance, but the practicality of the existing ORAM constructions is still questionable. Firstly, the existing ORAM constructions still require either large bandwidth consumption or storage capacity. Secondly, these ORAM constructions all assume a single user mode, which has limited the application to more general, multiple user scenarios.

In this presentation, we aim to address the above limitations by proposing four new ORAM constructions:

- S-ORAM, which adopts piece-wise shuffling and segment-based query techniques to improve the performance of data shuffling and query through factoring block size into design;
- KT-ORAM, which organizes the server storage as a k-ary tree with each node acting as a fully-functional PIR storage, and adopts a novel delayed eviction technique to optimize the eviction process;
- GP-ORAM, a general partition-based ORAM that can adapt the number of partitions to the available user-side storage and can outsource the index table to the server to reduce local storage consumption; and
- MU-ORAM, which can deal with stealthy privacy attack in the application scenarios where multiple users share a data set outsourced to a remote storage server and meanwhile want to protect each individual's data access pattern from being revealed to one another.

We have rigorously quantified and proved the security strengths of these constructions and demonstrated their performance efficiency through detailed analysis.

IOWA STATE UNIVERSITY
Department of Computer Science